Annapolis Police Department

GENERAL ORDER

Number: I.5

Issue Date: July 2009

TO: All Personnel

SUBJECT: Mobile Data Terminals (MDT's)

PURPOSE

The purpose of this General Order is to define the use of the Mobile Data Terminals (MDT's) and handheld computers (pocket PC's).

POLICY

It shall be the policy of the Annapolis Police Department to use the Mobile Data Terminals and handheld computers (pocket PC's) to support the Department's activities. It is the responsibility of each member to ensure that this technology is used for proper business purposes and in a manner that does not compromise the confidentiality, protected, restricted or other sensitive information.

The Commander of the Support Services Division will designate an MDT Program Coordinator. The MDT Program Coordinator will conduct random administrative security checks of the MDT system and handheld computers (pocket PC's) to ensure that all necessary security procedures are being followed. The MDT Program Coordinator or his/her designee will also ensure that required members are trained on the proper use of the Mobile Data Terminals and handheld computers. For purposes of this policy handheld computers (pocket PC's) are also considered MDT's. The handheld computers have capabilities such as but not limited to check for wanted persons and to connect with the Motor Vehicle Administration.

I. General System Usage

A. All MDT's, data and software, maintained or used by the Annapolis Police Department are for official use only. No member will use or cause to be used any MDT's for personal gain or benefit of any kind.

B. No member will attempt to install unauthorized software programs or other files and/or delete or modify any software or hardware associated with the Mobile Data

Terminals. This also includes prohibiting the manipulation or alteration of current software running on agency owned MDT's. The configuration of the desktop monitor is also prohibited without authorization from the MDT Program Coordinator.

C. For service issues contact the MDT Program Coordinator.

II. Mobile Data Terminals (MDT's)

A. All electronic messaging/correspondence is the property of the Annapolis Police Department.

B. Use of Equipment

1. All traffic transmitted using the Mobile Data Terminals (MDT's) must be business related and comply with the same quality standards as voice traffic. Offensive, demeaning or disruptive messages are prohibited. **Any message containing slang or language that could be construed as a slur or sexual harassment against any person or group will not be tolerated.** All transmissions are recordable, retrievable and are public record.

2. The only personnel authorized to operate a Mobile Data Terminal are those specifically trained in its proper operation. Only those personnel who are MILES (Maryland Inter Agency Law Enforcement System) and NCIC (National Crime Information System) certified are authorized to access MILES and NCIC.

3. Members operating vehicles equipped with the MDT's must remember to give full time and attention to the operation of the vehicle.

4. Members will keep the Mobile Data Terminal, screen and keyboard clean using the supplies provided. Food and liquids must be kept away from the MDT's at all times. In the event of an accidental spillage, the member will:

   a. Log off all active sessions and shut down the Mobile Data Terminal as quickly as possible.
   b. Clean the affected area.
   c. Notify the MDT Program Coordinator as soon as possible to inspect the unit.

5. When away from the vehicle, members must ensure that the vehicle is locked to prevent unauthorized use of the Mobile Data Terminal. Members must ensure that handheld computers are secured to prevent theft/unauthorized use of the handheld computer.

6. Member's passwords to access the MDT's, and MILES/NCIC shall not be shared or made known to any other individuals. Members who believe that their password has been compromised shall immediately notify the MDT

Program Coordinator and change their password. Attempts by any member to utilize a MDT or gain access to MILES/NCIC with another member's password is prohibited.

III. Email and Internet Usage

A. Internet services that are used during working and non-working hours are for authorized purposes only. This may include but not be limited to using the Internet to train personnel on the use of the Internet, etc.

B. Members may use the Internet as a way to exchange information with the public and internally as an technology information tool.

1. Members will take adequate precautions when processing or storing data on computers connected to the Internet and when transferring data on or through the Internet. Information security requirements shall always be a primary consideration when utilizing the Internet.

2. The Internet **may not** be used for:

a. The pursuit of private, commercial business activities or profit-making ventures;

b. Matters directed towards any political candidate, special interest group, event or any political or social position;

c. Direct or indirect lobbying;

d. Use of Internet sites that result in additional charges to the Department.

e. Engaging in prohibited discriminatory conduct;

f. Obtaining or viewing sexually explicit material unless directly pursuant to an actual law enforcement purpose/investigation and then only with the prior permission of the members immediate supervisor;

g. Any activity that would bring discredit on the Department; and

h. Any violation of statute or regulation.

3. Personal use of email from an MDT is strictly prohibited.

IV. Training

A. Training on the MDT's will be conducted for new officers during GAP or during Field Training.

B. Officers who are MILES and NCIC certified will be recertified according to MILES and NCIC guidelines.

Michael A. Pristoop
Chief of Police

References
1. Accreditation Standard 41.3.7

Revision: This General Order replaces General Order I.5 dated April 2007